IN THE CLAIMS

For the convenience of the Examiner, all pending claims of the Application are reproduced below.

1. **(Previously Presented)** A method of preventing undesirable activities of Executable Objects via an application, comprising:

denying one or more threads of an application access to a secured resource if said one or more threads has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource; and

denying said one or more threads of the application Internet behavior if, at a time access is sought to the Internet, said one or more threads is accessing a secured resource.

2. **(Previously Presented)** A method according to Claim 1, further comprising recording in a memory events representative of Internet behavior, keeping a record of all secured resources that are to be kept secured and when an application that has previously exhibited Internet behavior attempts to access one such secured resource, denying access to said secured resource, unless:

a) At least a predetermined period of time has passed since a last Internet behavior; or

b) Said application, or one or more of its threads, has performed at least a predetermined number of operations after exhibiting Internet behavior; or

c) Another preset condition has been fulfilled.

3. **(Previously Presented)** A method according to Claim 2, wherein the preset condition comprises an exercise of control over execution of downloadables received during Internet behavior, to ensure that no unexecuted downloadable may access the secured resource.

4. **(Previously Presented)** A method according to Claim 2, wherein the present condition comprises an analysis of downloadables to ascertain the downloadables are harmless.

5. **(Previously Presented)** A method according to Claim 1, wherein Internet behavior is denied by disabling a network connection creation.

6. **(Previously Presented)** A method according to Claim 1, wherein Internet behavior is denied by disabling specific protocols.

7. **(Previously Presented)** A method according to Claim 6, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

8. **(Previously Presented)** A method according to Claim 1, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

9. **(Previously Presented)** A method according to Claim 5, wherein access to trusted sites is not denied.

10. **(Previously Presented)** A method according to Claim 1, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

11. **(Previously Presented)** A method according to Claim 1, wherein all sub-threads of a thread that is denied access to a secured resource are also denied access to secured resources.

12. **(Previously Presented)** A method according to Claim 1, wherein all sub-threads of a thread that is denied Internet behavior are also denied Internet behavior.

13. **(Previously Presented)** An apparatus for preventing undesirable activities of Executable Objects via an application, comprising:

a memory for storing a record of Internet behavior of a plurality of applications; and

means for denying one or more threads of an application access to a secured resource if said one or more threads has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

14. **(Previously Presented)** An apparatus for preventing undesirable activities of Executable Objects via an application, comprising:

a memory of storing a record of Internet behavior of a plurality of applications; and

means for denying one or more threads Internet behavior if, at a time access is sought, said one or more threads is accessing a secured resource.

15. **(Previously Presented)** A system for preventing undesirable activities of Executable Objects via an application, comprising:

a computer on which one or more applications, each application having one or more threads, are to run, said computer being connectable to the Internet or Intranet, or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said one or more applications; and

means for denying one or more threads of an application access to a secured resource if said one or more threads has previously exhibited Internet behavior and has not met a specific condition for accessing said secured resource.

16. **(Previously Presented)** A system for preventing undesirable activities of Executable Objects via an application, comprising:

a computer on which one or more applications, each application having one or more threads, are to run, said computer being connectable to the Internet or Intranet or Extranet, said computer being provided with a memory for storing a record of Internet behavior of each of said one or more applications; and

means for denying one or more threads Internet behavior if, at a time Internet behavior is exhibited, said one or more threads is accessing a secured resource.

17. **(Canceled)**

18. **(Previously Presented)** A method according to Claim 2, wherein Internet behavior is denied by disabling a network connection creation.

19. **(Previously Presented)** A method according to Claim 3, wherein Internet behavior is denied by disabling a network connection creation.

20. **(Previously Presented)** A method according to Claim 4, wherein Internet behavior is denied by disabling a network connection creation.

21. **(Previously Presented)** A method according to Claim 2, wherein Internet behavior is denied by disabling specific protocols.

22. **(Previously Presented)** A method according to Claim 3, wherein Internet behavior is denied by disabling specific protocols.

23. **(Previously Presented)** A method according to Claim 4, wherein Internet behavior is denied by disabling specific protocols.

24. **(Previously Presented)** A method according to Claim 21 wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

25. **(Previously Presented)** A method according to Claim 22, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

26. **(Previously Presented)** A method according to Claim 23, wherein the specific protocols comprise HTTP, FTP, SMTP, or like communication protocol.

27. **(Previously Presented)** A method according to Claim 2, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

28. **(Previously Presented)** A method according to Claim 3, wherein Internet behavior is denied by disabling transfer of executable objects in communication protocols.

29. **(Previously Presented)** A method according to Claim 4, wherein Internet behavior is denied by disabling a transfer of executable objects in communication protocols.

30. **(Previously Presented)** A method according to Claim 1, wherein access to trusted sites is not denied.

31. **(Previously Presented)** A method according to Claim 2, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

32. **(Previously Presented)** A method according to Claim 3, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.

33. **(Previously Presented)** A method according to Claim 4, wherein access to a secured resource is denied by disabling a thread using a specific system service that is used to access the secured resource.